



الحمد لله معز الاسلام بنصره ومذل الشرك بقهره ومصرف الامور بأمره  
ومستدرج الكافرين بمكره الذي قدر الايام دولا بعدله وجعل العافية للمتقين  
بفضله والصلاة والسلام علي من أعلي الله منار الاسلام بسيفه وعلي اله  
وصحبه ومن تبعهم باحسان الي يوم الدين اما بعد ..

يُعد نظام **أندرويد** من أكثر أنظمة التشغيل المستهدفة ببرمجيات خبيثة  
" **Malware** " وأحصنة طروادة " **Trojan** " حيث أن عدد مستخدمي  
أجهزة أندرويد يتجاوز مئات الملايين وتوجد عشرات المتاجر والمواقع  
الإلكترونية التي تنشر تطبيقات أندرويد دون فحصها أو تحليلها مما يعرض  
أمن المستخدمين إلى مخاطر الاختراق ، **لذلك أصبح فحص ملفات APK**  
**التي تُنشر من قبل أطراف ثالثة أو أشخاص مجهولين ضرورة حتمية للحفاظ**  
**على أمنك الشخصي** فكما نُحذر دائماً من تحميل التطبيقات من المواقع  
الإلكترونية والمتاجر المشبوهة التي تروج لتحميل تطبيقات مدفوعة بشكل  
مجاني فتكون بياناتك ومعلوماتك هي الثمن الحقيقي من تثبيت تلك التطبيقات  
على جهازك فإننا ننصح بالإعتماد على تحميل البرمجيات من مصادرها  
الرسمية فقط

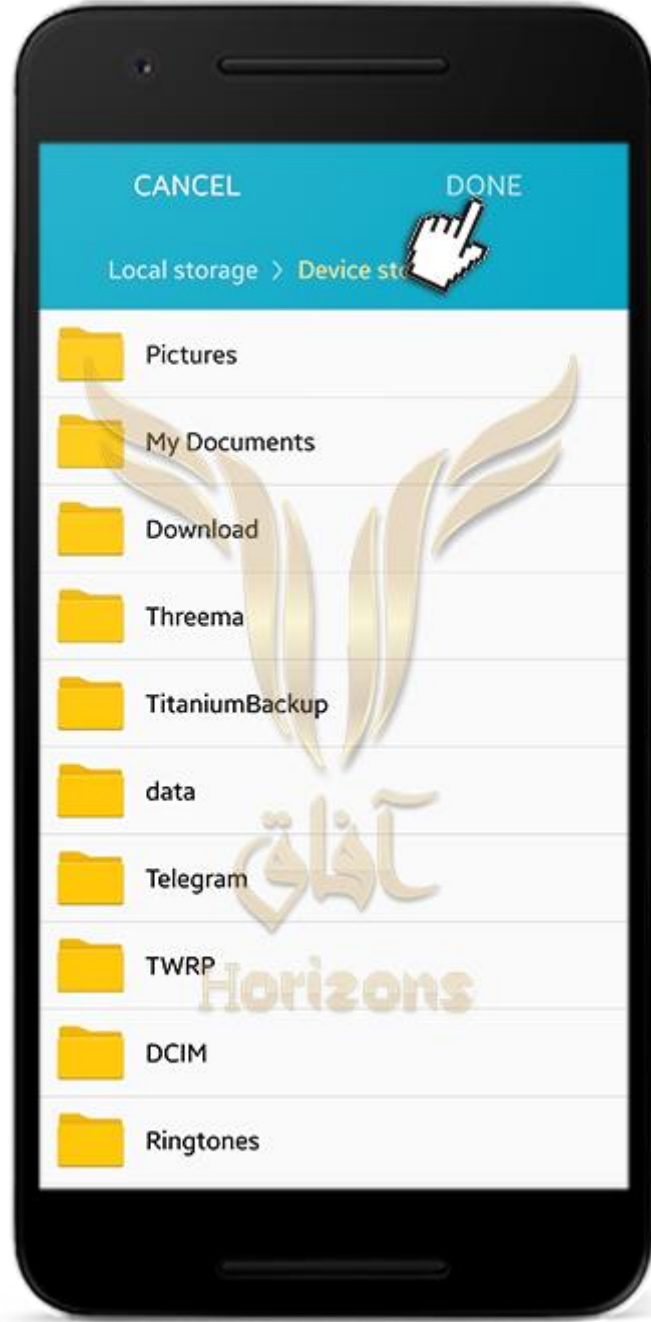


● أولاً توجه الى موقع الفحص [apkscan.nviso.be](https://apkscan.nviso.be)

● ثم اضغط على **choose file**



● واختر الملف المراد فحصه ثم اضغط على **DONE**



● وانتظر حتى الانتهاء من رفع الملف إلى الموقع



● بعد انتهاء رفع الملف اضغط على **scan package** لبدء الفحص  
وانتظر حتى تظهر النتيجة

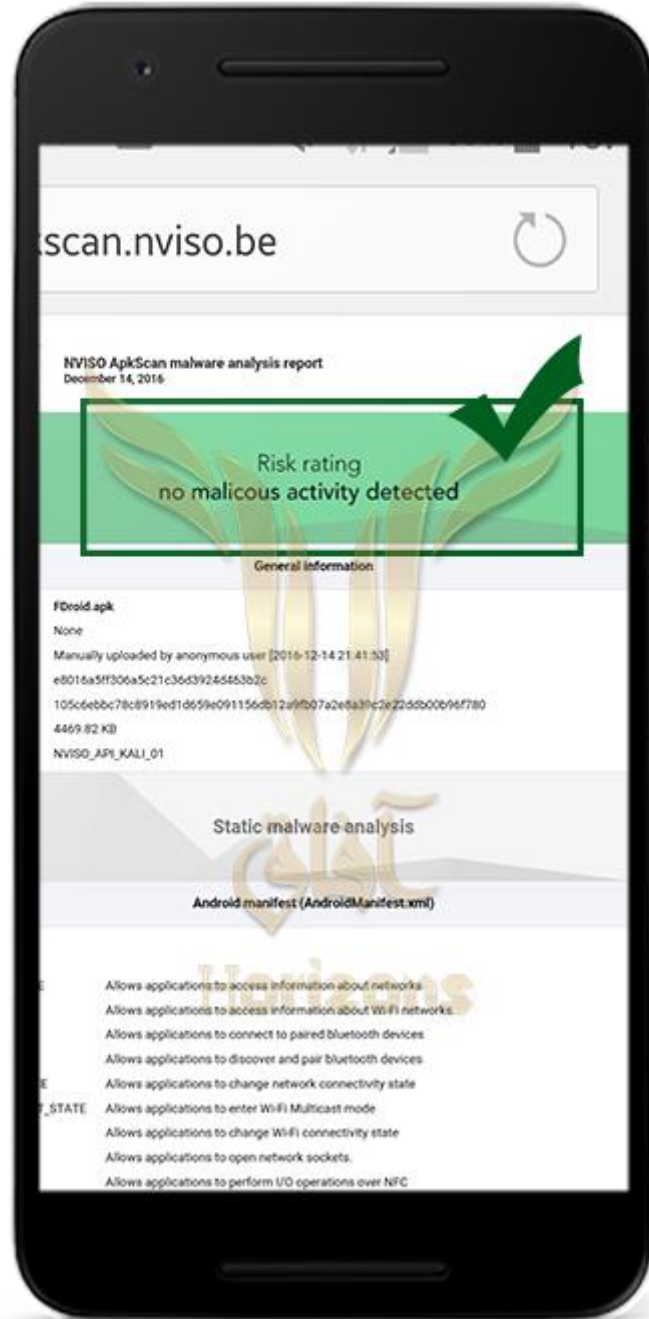
**توضيح**

يمكنك متابعة النتيجة عن طريق البريد الالكتروني الذي سيصلك خلال **email me the results when scan has finished** دقائق بعد انتهاء الفحص فاذا اردت ذلك فعّل خيار



● اذا ظهرت عبارة **No Malicious Activity Detected** فذلك يعني أن الملف سليم ✓





● وإذا ظهرت عبارة **Confirmed Malicious** فيعني أن الملف ملغم ⚠





## NVISO AppScan malware analysis report

December 14, 2018

Risk rating  
confirmed malicious

### General information

File name	OFFSE.apk
Other known file names	None
Origin	Manually uploaded by anonymous user [2018-12-14 21:47:56]
MD5 hash	2e011c0d50c2940058f80061180ff5
SHA256 hash	8f6a8770700a28713e722d0e70a0605d39507b0409638174b41c0d0c193f
File size	244 KB
Vendor	ROMAN_KALININ

### Static malware analysis

#### Android manifest (AndroidManifest.xml)

#### Permissions

ACCESS_FINE_LOCATION	Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi.
ACCESS_NETWORK_STATE	Allows applications to access information about networks.
ACCESS_WIFI_STATE	Allows applications to access information about Wi-Fi networks.
CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm being dialed.
CAMERA	Required to be able to access the camera device.
CHANGE_NETWORK_STATE	Allows applications to change network connectivity state.
CHANGE_WIFI_STATE	Allows applications to change Wi-Fi connectivity state.
GET_TASKS	Allows an application to get information about the currently or recently running tasks.
INTERNET	Allows applications to open network sockets.
READ_CALL_LOG	Allows an application to read the user's call log.
READ_CONTACTS	Allows an application to read the user's contacts data.
READ_EXTERNAL_STORAGE	Allows an application to read from external storage.
READ_HISTORY_BOOKMARKS	Allows an application to read (but not write) the user's browsing history and bookmarks.
READ_PHONE_STATE	Allows read-only access to phone state.
READ_SMS	Allows an application to read SMS messages.
RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting.
RECORD_AUDIO	Allows an application to record incoming SMS messages to record or perform processing on them.
RECORD_AUDIO	Allows an application to record audio.

#### Services

Class net.briqack.server.Controller  
Class net.briqack.server.GPSLocation  
Class net.briqack.server.Toast  
Class net.briqack.server.Controller  
Class net.briqack.server.GPSLocation  
Class net.briqack.server.Toast



### توضيح

اسفل الشريط ستجد العديد من البيانات الاخرى الخاصة بنتيجة الفحص مثل  
" Malware " اسماء المكافحات التي رصدت الملف كبرمجية خبيثة

=====

## 📖 | قد يهمك أيضاً

- الأرشيف التقني
- دليل الحماية الإلكترونية للهواتف الذكية
- دورة احتراف لينكس منت
- دورة أمن الهواتف الذكية
- خدمات الـ VPN
- الحماية من تسريبات المتصفح
- دورة أمن الحاسوب

**واخر دعوانا ان الحمد لله رب العالمين**



Horizons

مؤسسة افاق الإلكترونية

**للتواصل**



@TECH\_SUPPORT



@SR444TAW